WebKitGTK+ Security Status

Michael Catanzaro

Igalia S.L.

November 11-12, 2015

Outline

WebKit1 Compatibility Packages

- All distros have TWO WebKitGTK+ packages
  - WebKitGTK+ 2.4 package, for WebKit1 API compatibility
  - A newer WebKitGTK+ package (2.10.x, 2.8.x, or 2.6.x)
- Very many apps are stuck on 2.4
- Last real security updates for 2.4 were in January

Safari Security Advisories

- "Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution"
- Eight advisories in 2015
- 113 2015 CVEs (discounting Safari CVEs)

WebKitGTK+ Security Advisory WSA-2015-0001

- January 26, 2015
- 41 reported CVEs
- Covers 2.4 series before 2.4.8

WebKitGTK+ Security Updates

- No CVEs
- No security advisories
- Security bugs fixed in trunk are regularly backported to the latest stable series (2.10).
- So if distros ship our releases, users will get the fixes.
- What versions of WebKitGTK+ are shipped in popular distros?

- WebKitGTK+ 2.10.3 (latest version)

Fedora

- Fedora 23: WebKitGTK+ 2.10.3 (latest version)
- Fedora 22: WebKitGTK+ 2.8.5
- Fedora 21: WebKitGTK+ 2.6.6

Debian

- Debian 8: WebKitGTK+ 2.6.2, plus patch for CVE-2015-2330
- Debian 7: WebKitGTK+ 1.8.1

"Debian 8 includes several browser engines which are affected by a steady stream of security vulnerabilities. The high rate of vulnerabilities and partial lack of upstream support in the form of long term branches make it very difficult to support these browsers with backported security fixes. Additionally, library interdependencies make it impossible to update to newer upstream releases. Therefore, browsers built upon the webkit, qtwebkit and khtml engines are included in Jessie, but not covered by security support. These browsers should not be used against untrusted websites."

Ubuntu

- Ubuntu 15.10: WebKitGTK+ 2.8.5 (in universe)
- Ubuntu 15.04: WebKitGTK+ 2.6.2, plus patch for CVE-2015-2330 (in universe)
- Ubuntu 14.04 LTS: WebKitGTK+ 2.4.8 (originally 2.4.0!)

- openSUSE 42.1: WebKitGTK+ 2.8.5
- openSUSE 13.2: WebKitGTK+ 2.6.6
- openSUSE 13.1: WebKitGTK+ 2.2.7

Enterprise Distros

- RHEL 7: WebKitGTK+ 2.0.4
- SLE: WebKitGTK+ 2.4.8, plus patch for CVE-2015-2330

Solution?

- We must release a list of CVEs fixed in each version of WebKitGTK+ or users will not get our updates.
  - If there's no CVE, it's not a security issue.
  - Maybe not essential that the CVEs be immediately available
- Options:
  - Reuse CVEs issued by Apple (we need help to do this!)
  - Request our own CVEs for each issue

Sandboxing

- WebKit sandbox only works on OS X (and iOS?)
- seccomp filters sandbox for Linux in trunk, but experimental
- Development stalled because seccomp filters seem risky
- seccomp filters are used in Chrome's sandbox, but only as one layer, and Chrome bundles its dependencies.

HTTPS Achievements

- Rapidly disabled SSL3 after POODLE
- Disabled RC4 over a year before other browsers

HTTPS Problems

- No support for HSTS
- No support for HPKP
- No support for certificate transparency
- No detection of SHA-1 signatures
- No detection of weak DH primes (all above 728 bits allowed by GnuTLS)

Summary

- Updates: very, but releasing CVEs would make things much less bad
- Sandbox: exists, but experimental (disabled by default)
- HTTPS: falling behind